PATENT ABSTRACTS OF JAPAN

(11)Publication number : **03-179841**
(43)Date of publication of application : **05.08.1991**

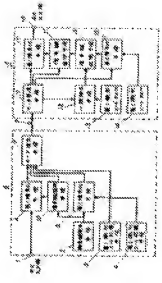
(51)Int.Cl. **H04L 9/06**
G09C 1/00
H04L 9/14
H04N 7/167

(21)Application number : **02-282076**
(22)Date of filing : **19.10.1990**

(71)Applicant : **MATSUSHITA ELECTRIC IND CO LTD**
(72)Inventor : **EJIMA NAOKI**

(54) CRYPTOGRAPHIC DIGITAL BROADCAST RECEIVER

(57)Abstract:
PURPOSE: To deliver individual information individually and safely with remote control at sender side by specifying a receiver with an identification code and ciphering and decoding information such as a key table required to decode an individual contract program while applying remote control individually.
CONSTITUTION: A 2nd decoding means 15 receiving a data broadcast through a transmission line 9, extracting a data corresponding to an identification code and collating the data with a data of an identification code ROM 13 and decoding a decoding key or a decoding key group revising the received data at a low speed is provided. Moreover, a decoding key reproducing means 21 extracting a 1st key or a key group revised at a high speed from the received data and reproducing a substantial decoding key from the key and the decoding key or decoding key group and a 1st decoding means 17 or the like decoding the received cryptographic sentence under the substantial decoding key are provided. Thus, the privacy call processing and ciphering with high safety without signal deterioration are applied and the operation of specific channel and specific receivers is controlled remotely from the sender side in response to the content of contract.



⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平3－179841

⑤Int. Cl.⁵	識別記号	庁内整理番号	㊸公開　平成3年(1991)8月5日
H 04 L 9/06			
G 09 C 1/00		7343－5B	
H 04 L 9/14			
H 04 N 7/167		8725－5C	
		6914－5K	H 04 L 9/02　Z
			審査請求　有　発明の数 1　（全6頁）

⑭発明の名称　暗号デジタル放送受信装置

㉑特　願　平2－282076
㉒出　願　昭58(1983)11月16日
㉓特　願　昭58－215410の分割

㉗発　明　者　江　島　　直　樹　大阪府門真市大字門真1006番地　松下電器産業株式会社内
㉑出　願　人　松下電器産業株式会社　大阪府門真市大字門真1006番地
㉔代　理　人　弁理士　小銀治　明　外2名

明　細　書

1、発明の名称

暗号デジタル放送受信装置

2、特許請求の範囲

低速に更新される第２の鍵または鍵群を受信装置に固有の識別コードで個別に暗号化して配送する手段と、高速に更新される第１の鍵または鍵群を前記第２の鍵または鍵群で暗号化して複数の受信装置に共通に放送する手段と、前記第１の鍵または鍵群を用いて平文を暗号化して放送する手段を備えた暗号デジタル放送装置の放送信号を受信する受信装置であって、

伝送路を通じて放送されるデータを受信する手段と、受信装置に予め付与する個別の識別コードを蓄積する識別コードＲＯＭと、受信データから前記識別コードに相当するデータを取り出して前記識別コードＲＯＭのデータと照合する一致検出手段と、受信データから低速に更新する第２の鍵または鍵群を前記識別コードＲＯＭのデータを用いて解読して復号鍵または復号鍵群を得る第２の復号化手段と、前記第２の復号化手段で得られる復号鍵または復号鍵群を格納する記憶手段と、受信データから高速に更新する第１の鍵または鍵群を取り出してこれと前記復号鍵または復号鍵群とから実質の復号鍵を再生する復号鍵再生手段と、前記復号鍵再生手段から出力する実質の復号鍵の下に受信した暗号文を復号化する第１の復号化手段を備える暗号デジタル放送受信装置。

3、発明の詳細な説明

産業上の利用分野

本発明は有料のＣＡＴＶ（ケーブル・テレビ・システム）や、有料の商品放送システムに利用できる暗号デジタル放送受信装置に関する。

従来の技術

従来の有料放送システムでは非公開の特定のフォーマットによるものや、秘話化を施して盗視聴を防止しようとするものがあった。アナログでの秘話化はベースバンド信号を変換手段で加工し、受信機器で逆変換回路を働かせて元の信号に戻すようにしていた。例えば、映像同期信号を時々反

転する方法等がある。

発明が解決しようとする課題

このような従来技術では、秘話のアルゴリズムが変えれ易く、盗視聴が比較的簡単であった。また、秘話にともなって信号が劣化する等の課題がある。しかも、送信側から特定の信号を送出して個別の受信機の動作を遠隔制御する機能を実現することが困難であった。

本発明はこの問題点に鑑み、有料のデジタル放送において、信号劣化がなく、安全性の高い秘話化，暗号化を行い、契約内容に応じて特定のチャンネルや特定の受信機器の機能動作を送信側から遠隔制御可能なシステムに利用する暗号デジタル放送受信装置を提供することを目的とする。

課題を解決するための手段

上記従来の問題を解決するために本発明の暗号デジタル放送受信装置は、伝送路を通じて放送されるデータを受信する手段と、受信装置に予め付与する個別の識別コードを蓄積する識別コードROMと、受信データから前記識別コードに相当するデータを取り出して前記識別コードROMのデータと照合する一致検出手段と、受信データから低速に更新する第2の鍵または鍵群を前記識別コードROMのデータを用いて解読して復号鍵または復号鍵群を得る第2の復号化手段と、前記第2の復号化手段で得られる復号鍵または復号鍵群を格納する記憶手段と、受信データから高速に更新する第1の鍵または鍵群を取り出してこれと前記復号鍵または復号鍵群とから実質の復号鍵を再生する復号鍵再生手段と、前記復号鍵再生手段から出力する実質の復号鍵のFECで受信した暗号文を復号化する第1の復号化手段を備えたものである。

作　用

本発明は上記の構成により、暗号デジタル放送装置で、平文の暗号化に使用する低速に更新する暗号鍵または暗号鍵群を、識別コードで特定する受信装置へ、それぞれ識別コードで個別に暗号化した上で送出するようにし、平文は高速に更新する暗号鍵または暗号鍵群を低速に更新する第2の暗号鍵で暗号化して放送された放送信号を、伝送路を通じて受信した時、本発明の暗号デジタル放送受信装置は、伝送路を通じて受信したデータから識別コードを取り出し、受信装置に予め個別に付与された識別コードROMのデータと照合する。照合の結果符合していれば、識別コードROMのデータを用いて受信した低速の伝送鍵または伝送鍵群を第2の復号化手段で解読する。第2の復号化手段から出力された復号鍵または復号鍵群を復号鍵記憶手段へ格納する。一方、照合の結果不一致であれば、他の受信装置へのデータであるとして、受信した伝送鍵のデータを捨て記憶手段へ取り込まない。

受信したデータから高速に更新する第1の鍵または鍵群を取り出し、復号鍵記憶手段のデータで復号化して実質の復号鍵として出力する。受信した暗号文を実質の復号鍵で復号化し、平文を出力するよう動作する。

復号鍵記憶手段に復号鍵または復号鍵群が正しく格納されていない場合には、受信した暗号文は不正に復号化され、あるいは復号化されないので、平文とは異なるものを出力するよう動作する。

実　施　例

以下、本発明の一実施例について、図面を参照しながら説明する。図は本発明の一実施例による暗号デジタル放送装置および暗号デジタル放送受信装置のブロック図を示すものである。

図において、1は平文入力端、2は暗号鍵発生手段、20は暗号鍵選択手段、3は第1の識別コード記憶手段、4は第2の識別コード記憶手段、5は第2の暗号化手段、9は第1の暗号化手段、7はデータ送出手段、8は前記した平文入力端1からデータ送出手段8までと暗号鍵選択手段20を複合した暗号デジタル放送装置である。

また、9は伝送ケーブル、11はデータ受信手段、12は一致検出手段、13は第1の識別コードROM、14は第2の識別コードROM、15は第2の復号化手段、16は復号鍵記憶手段、21は復号鍵選択手段、17は第1の復号化手段、18は平文の出力端、19は前記したデータ受信手段11から平文の出力端18までと復号鍵選択手段

２１を複合した暗号デジタル放送受信装置である。

以上のように構成された本実施例の暗号デジタル放送装置および暗号デジタル放送受信装置の動作について、以下、システムの概略から順に説明する。

暗号デジタル放送装置８は伝送ケーブル９を中継して複数の暗号デジタル放送受信装置に接続されている。図に示す暗号デジタル放送受信装置19は、そのうちの１つである。暗号デジタル放送受信装置１９には、個別の識別コードを機器を製造し出荷する時点で設定しておく。第１の識別コードＲＯＭ１３及び第２の識別コードＲＯＭ１４がこれに相当する。識別コードはシステムを管理する組織が作成する。機器の使用者または契約者とシステム管理者の契約が交わされると、新たな契約内容がデータファイルに書き込まれ、更新される。暗号デジタル放送装置８は、全契約者の最新の契約内容データをアクセスできるよう第１の識別コード記憶手段３と第２の識別コード記憶手段４にそのデータを格納しておく。平文入力端１に入力された番組は第１の暗号化手段６で暗号化してデータ送出手段７から送出・放送される。

第１の暗号化手段６で使用する暗号鍵は放送せずに、暗号鍵選択手段２０で選択された暗号鍵の索引番号が番組とともにデータ送出手段７から放送される。すべての索引番号と暗号鍵の対応関係を表す鍵テーブルは暗号鍵発生手段２で作成される。暗号鍵発生手段２で作成した鍵テーブルは暗号鍵選択手段２０及び第２の暗号化手段５に供給する。暗号鍵選択手段２０によって鍵テーブルの中から１つの索引番号を選択してこの索引番号をデータ送出手段７へ供給するとともに、鍵テーブルを参照して、その中から索引番号の暗号鍵を選択し第１の暗号化手段６へ出力する。この暗号鍵を用いて第１の暗号化手段６は平文入力端１から入力した平文を暗号化して暗号文を作成しデータ送出手段７へ供給する。なお、暗号鍵選択手段２０で選択する索引番号および暗号鍵は、盗視聴を防止するために乱数を利用して時々刻々１秒に数回程度更新する。また、暗号鍵発生手段２で作成する鍵テーブルも低速に更新される。

暗号デジタル放送受信装置１９では、番組放送に先だって鍵テーブルを準備しておく必要がある。鍵テーブルは契約対象の機器にだけ配送する。この配送のために番組と別のルート、衛星波、チャンネルを占有するのは不経済なので、番組と同一のチャンネルを時分割多重して配送する。また、鍵テーブルが第３者に知れると不正な盗視聴をされる危険があるので、配送には安全性が確保されなければならない。しかも、それぞれの機器で異なる契約に応じて異なった鍵テーブルを、その対象の機器にだけ安全に配送するために、個別の機器毎に異なる暗号化を行う。以下、この暗号化について説明する。

暗号デジタル放送受信装置個別の識別コードは機器を特定するための第１の識別コードと、暗号鍵として用いる第２の識別コードを含むように設定されている。なお、第２の識別コードは第１の識別コードと対応づけてシステム管理者が一意に決定するが、第２の識別コードから第１の識別コードが求められるとは限らないように作成される。第１の識別コードと第２の識別コードはそれぞれ第１の識別コード記憶手段３および第２の識別コード記憶手段４に全契約者のデータが格納されている。

安全配送のために個別の機器毎に行う鍵テーブルの暗号化は、第２の識別コード記憶手段４から取り出した第２の識別コードを暗号鍵として、第２の暗号化手段５において行われる。こうして作成されたものを伝送鍵テーブルという。従って、鍵テーブルが同一であっても第２の識別コードが異なれば、これによって暗号化された伝送鍵テーブルは個々の機器で異なったものとなる。伝送鍵テーブルの作成は順次行い全ての契約機器について行う。これらのデータを使って、１つの契約機器に対する鍵テーブルの配送は、第１の識別コードと伝送鍵テーブルをパックにして他のデータとともにデータ送出手段７から送出することで行われる。１つの契約機器に対する鍵テーブルの配送が終了したら、次の契約機器についてというように、

配送は原次シリアルに行い全ての契約機器にくまなく鍵テーブルを配送する。第２の鍵または鍵部の更新は低速なので、少なくとも全ての契約機器に配送が完了するまでの期間は更新されない。伝送エラーや受信機器の電源未投入などを考慮して、配送は繰り返される。

以上述べた、暗号文，索引番号，第１の識別コードおよび伝送鍵テーブルは、時系列にあるいはデータフォーマット上において互いに関連づけてデータ送出手段７に入力される。データ送出手段７では、これらのデータを実調に好適なフォーマットとし、ＰＳＫ変調したＶＨＦ帯の搬送波に乗せて伝送ケーブル９へ出力する。伝送ケーブル９はシステムの規模によって、リンク，中継，分配を行って最終需要家の暗号デジタル放送受信装置へ接続される。暗号デジタル放送受信装置１９はそのうちの１つである。

以上のようなシステムで構成される放送系において、本発明の暗号デジタル放送受信装置の実施例の動作について説明する。

暗号デジタル放送受信装置１９では、伝送ケーブル９を通じてデータ受信手段１１で多重データを受信する。受信した多重データはデータ受信手段１１から内容に従ってそれぞれ出力する。多重データから取り出した第１の識別コードと、受信装置に予め個別に付与された第１の識別コードＲＯＭ１３のデータとは、一致検出手段１２によって照合される。照合の結果符合していれば、データ受信手段１１で受信したデータから取り出した伝送鍵テーブルを第２の識別コードＲＯＭ１４のデータを復号鍵として第２の復号化手段１５で解読し、復号済みの鍵テーブルを復号鍵記憶手段１６へ格納する。こうして、配送される鍵テーブルの受信が完了する。格納された復号済みの鍵テーブルは復号鍵選択手段２１に供給する。

多重データから取り出した第１の識別コードと、第１の識別コードＲＯＭ１３のデータとが、一致検出手段１２によって照合された結果、不一致であれば、そのパックデータは他の受信装置へのデータであるとして、受信した鍵テーブルのデータを捨て、復号鍵記憶手段１６への格納を禁止する。この場合、鍵テーブルの受信が未完であるが、鍵テーブルは原次繰り返して配送されるので、次に自身の第１の識別コードが送出されるのを待つ。

一方、受信した多重データから取り出した暗号鍵の索引番号を復号鍵選択手段２１へ供給し、復号鍵記憶手段１６から入力された復号済みの鍵テーブルを参照して、その中から索引番号の復号鍵すなわち実質の復号鍵を選択し第１の復号化手段１７へ出力する。

また、受信した多重データから取り出した暗号文を第１の復号化手段１７へ供給し、復号鍵選択手段２１から入力された実質の復号鍵を使用して第１の復号化手段１７で復号化し、平文を平文の出力端１８へ出力するよう動作する。このようにして、正規に契約している受信装置の、暗号解読がなされ、番組が正しく復号化され、サービスが行われる。

配送される鍵テーブルの受信が未完である場合には、自身の第１の識別コードが送出されるのを待って、その後鍵テーブルの受信が完了したら、上述した動作によって正規のサービスが行われる。

番組放送の時点でも、なお配送される鍵テーブルの受信が未完である場合には、索引番号は受信できてもそれに対応する復号鍵が不明であるので、第１の復号化手段１７において、受信した暗号文が不正に復号化され、あるいは全く復号化されないので、出力端１８の出力は平文とは異なるものが出力され、番組のサービスを受けられないように動作する。このような場合、出力をミュートする。

従って、番組サービスが受けられないのは次のような種々の場合がある。

(ｱ) 未契約機器の場合、受信機器の第１の識別コードが放送されないので動作しない。

(ｲ) 契約機器であって当該番組あるいはチャンネルが未契約である場合、鍵テーブルの当該番組に使用する一部が未配送なので、その番組あるいはチャンネルに限って動作しない。

(ｳ) 契約期間が過ぎ未更改の場合、第１の識別

コードの放送を停止するか、または鍵テーブルに正しくないデータを配送するので、受信機器の動作が停止する。

また本発明の実施例とは異なるが、監視聴機器の場合の動作について説明する。

(ヒ) 不正規の監視聴機器の場合、放送データ（伝送鍵テーブル）から鍵テーブルを盗むことは不可能であるので、監視聴の動作はできない。

(ト) 不正規の監視聴機器であって鍵テーブルを不正に入手した場合、鍵テーブルが所定期間後に更新されるので、それ以降は監視聴の動作が停止する。

(チ) 不正規の監視聴機器であって、第１の識別コードROMおよび第２の識別コードROMを正規の契約機器から不正にコピーした場合、監視聴機器は契約機器のクローンとなるが、定期的に実施する点検時に第２の識別コードROMを交換するなどのメンテナンスをすれば、それ以降は監視聴の動作が停止する。

なお、以上の実施例では第１の識別コードROMと第２の識別コードROMを独立の構成手段としたが、これらと等価な識別コードROMとして一体としてもよいことは言うまでもない。

また、鍵テーブルは１つの鍵でもよく、この場合には索引番号に相当するデータによってさらに暗号化・復号化をするようにしてもよいことは、図面と以上の説明から明白である。すなわち、実施例で述べた鍵テーブルは鍵または鍵群と等価なものである。

発明の効果

以上の説明から明らかなように本発明は、暗号デジタル放送装置および暗号デジタル放送受信装置に識別コードを共有すること、その識別コードで受信装置を特定して個別に遠隔制御しながら、個別の契約番組を復号するに要する鍵テーブル（第２の鍵または鍵群）等の情報を暗号化・復号化するように構成したので、送信側の遠隔制御で特定の契約機器にこれらの個別の情報を個別に、安全に、配送することができる。

また、暗号鍵をランダムかつ頻繁に切り換えるようにできるので、伝送文を盗視聴して一時のデータについて不正に解読したとしても継続して解読することはほとんど不可能であり、すなわち暗号文の秘話能力が極めて高いという効果がある。

また、正規の契約機器の復号に必要な鍵テーブルは、個別の機器毎に異なる識別コードで暗号化して伝送鍵テーブルに変えて配送するので、伝送鍵テーブルは個々の機器で異なったものとなる。従って、他人の伝送鍵テーブルを盗んだとしても解読することがほとんど不可能である。このように、鍵テーブルの配送が個別の暗号デジタル放送受信装置に対して可能であり、しかも、極めて安全に配送され受信できるという効果がある。

なお、暗号化はデジタルで行われるので、復号信号の特性劣化がないことは、言うまでもない。

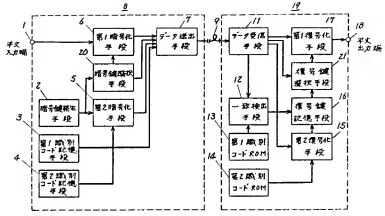
以上のように本発明は、例えば、ＣＡＴＶの有料デジタル放送、衛星による有料放送、地上波の空きチャンネルを活用する有料放送に利用し得る優れた暗号デジタル放送受信装置を実現できるものである。

４、図面の簡単な説明

図面は本発明の一実施例による暗号デジタル放送装置および暗号デジタル放送受信装置のブロック図である。

１……平文入力端、２……暗号鍵発生手段、２０……暗号鍵選択手段、３……第１の識別コード記憶手段、４……第２の識別コード記憶手段、５……第２の暗号化手段、６……第１の暗号化手段、７……データ送出手段、８……暗号デジタル放送装置、９……伝送ケーブル、１１……データ受信手段、１２……一致検出手段、１３……第１の識別コードROM、１４……第２の識別コードROM、１５……第２の復号化手段、１６……復号鍵記憶手段、２１……復号鍵選択手段、１７……第１の復号化手段、１８……平文の出力端、１９……暗号デジタル放送受信装置。

代理人の氏名　弁理士　小鍜治　明　ほか２名


8
19
1
6
7
9
11
17
18
平文入力端
第1暗号化手段
データ送出手段
データ受信手段
第1復号化手段
平文出力端
10
暗号鍵設定手段
20
21
2
5
12
復号鍵選択手段
暗号鍵発生手段
第2暗号化手段
一致検出手段
16
復号鍵記憶手段
3
13
15
第1識別コード記憶手段
第1識別コードROM
第2復号化手段
4
14
第2識別コード記憶手段
第2識別コードROM